Session #50

Don’t Be Tomorrow’s Headlines … Effective Measures for Protecting PII Data

START HERE GO FURTHER FEDERAL STUDENT AID®

Session #50

WELCOME

Richard Gordon
Chief Information Officer
Federal Student Aid

Session #50

Dick Boyle
President and CEO, ECMC Group

Dr. Danny Harris
Chief Information Officer, Department of Education

Cathy Hubbs
CISO, American University

Ira Winkler, CISSP
President, Internet Security Advisors Group

Session #50

ECMC Physical Data Theft: A Real-Life Case Study

Dick Boyle, President and CEO
ECMC Group

Incident Recap

- Physical theft of two 200-lb safes from a locked room in our secured headquarters.
- Safes included DVDs containing PII data on 3.3 million student loan borrowers.
- Data recovered within 36 hours (although ECMC was not notified for nearly 1 month).
- Significant cost.
- Significant impact.

Actions Taken

- Contacted law enforcement.
- Activated our incident response plan.
- Engaged crisis team that included key personnel from across the enterprise.
- Retained experts in data theft.
- Established guiding principles for managing the crisis.
- Worked closely with Department of Education.
- Arranged for credit monitoring and identity theft protection services for borrowers.

6 Recommendations

1. Be alert – it can happen to you!
2. Ensure each employee understands his/her role in protecting PII data.
3. Review your physical and data security controls.
4. Know where your data is; and ensure it is secure.
5. Ensure your policies are easily accessible and understandable to employees.
6. Be prepared in the event you are faced with a crisis.

Contact Information

If you have security-related questions for ECMC, please contact our Chief Security Officer.

Ron Kuriscak
651-325-4085
rkuriscak@ecmc.gov

Session #50

Combating Cyber Crime Through Securing PII

Building a Strong Awareness Program

Dr. Danny A. Harris
Chief Information Officer
Department of Education

START HERE
GO FURTHER
FEDERAL STUDENT AID®

For Official Use Only

Agenda

- Current State of Cyber Crime
- Defining PII
- The Importance of Awareness
- Building a Strong Awareness Program
- Building a Strong Awareness Program – Best Practices

Current State of Cyber Crime

- **500 Million** Sensitive Records Breached Since 2005
- **130 million** Credit cards stolen from Heartland Payment Systems in January 2009
- **130,000** Student records exposed in massive data breach at a large west coast university in January 2010
- **32,000** Since 2006, DoED customer computers have been victims of keyloggers over 32,000 times
- **Noticeable increase** of cybercrime activity targeting government compromise of PII for profit *(Source: US CERT, November 5, 2010)*

Current State of Cyber Crime

Top Ten Cyber Crime Complaints

- Non-delivery (paying for merchandise online, but not receiving it)
- Auction fraud
- Debit/credit card fraud
- Confidence fraud
- Computer fraud
- Check fraud
- Nigerian letter fraud
- Identity theft
- Financial institutions fraud
- Threats

Read more: http://www.brighthub.com/internet/security-privacy/articles/83739.aspx#ixzz14jDBjtiH)

Current State of Cyber Crime

Average Monetary Loss Per Fraud Complaint

- Debit/credit card fraud: $223.00
- Auction fraud: $610.00
- Non-delivery (merchandise and payment): $800.00
- Computer fraud: $1,000.00
- Nigerian letter fraud: $1,650.00
- Check fraud: $3,000.00

Read more: http://www.brighthub.com/internet/security-privacy/articles/83739.aspx#ixzz14jHpb4EK

What is PII?

Generally considered PII

- Full name (if not common)
- Telephone number
- Street address
- E-mail address
- IP address (in some cases)
- Vehicle registration number
- Driver's license number
- Biometrics
- Credit card numbers
- Digital identity
- SSN
- Military service numbers

Not generally considered PII

- First or last name, if common
- Country, state, or city of residence
- Age, especially if non-specific
- Gender or race
- Name of the school attended or workplace
- Employee name
- Grades, salary, or job position
- Criminal record

Importance of Awareness

Human error causes roughly 70% of the problems that plague data centers today. Whether it’s due to neglect, insufficient training, end-user interference, tight purse strings or simple mistakes, human error is unavoidable. The management of operations is your greatest vulnerability, but also is a significant opportunity to avoid downtime. The good news is people can be retrained.

From Computerworld, August 12, 2010

Building a Strong Awareness Program

- Establish Program Goals
- Develop Information Assurance Topics
- Develop Delivery Methods
- Establish Program Management

Building a Strong Awareness Program

Establish Program Goals

- To communicate and clarify organization’s overall intent to secure its information resources
- To provide information about security risks and controls
- To promote staff awareness of their responsibilities in relation to information security
- To motivate staff to comply with the organization’s security policy and procedures

Building a Strong Awareness Program

Develop Information Assurance Topics

- Information security policies
- Relevant laws
- Background information on fundamental information security concepts and issues
- News of significant security events
- Advice on maintaining home computer security
- Emerging information security risks
- Case studies

Building a Strong Awareness Program

Develop Delivery Methods

- Monthly emails
- Intranet delivery
- Newsletters
- Screensavers
- Brown bag workshops
- Security experts panel discussions
- Branding: link message together through logo, consistent styles, and format
- New employee orientation

Building a Strong Awareness Program

Establish Program Management

- Perform gap analysis to identify elements currently in place
- Develop tools and techniques to fill gaps
- Implement across organization
- Measure improvements through assessment tools
    - Monitor for compliance
    - Obtain feedback from stakeholders
- Maintain and update tools as program needs change

Strong Awareness Program Best Practices

Program/System Best Practices

- **Adequate protection:** Protect each customer's PII from inappropriate exposure or sharing.
- **Senior management commitment:** Senior management ensures that staff understands it is serious about protecting customer PII.
- **Transparency:** Inform customers about PII use and protection. Give customers information about what the Department is doing to protect their PII, how it will be used, and how it will be disposed.
- **Check and check again:** Protect customer PII through frequent inspections and audits.

Strong Awareness Program Best Practices

Program/System
Best Practices, continued

- **Only collect required PII:** Reduce duplicative requirements
- **Align people:**
  - Governance and accountability
  - Awareness and training
- **Establish Computer Matching Agreements:** Inter-agency PII sharing require Computer Matching Agreements
- **Adhere to local and state legal requirements:** There are at lease 48 separate implementations of the Privacy Act. It's important to know your jurisdictions requirements.

Strong Awareness Program Best Practices

Practitioner
Best Practices

- Recognize PII
- Stop, Think, Click
- Report breaches
- Transmit PII securely (encryption)
- Store securely
- Dispose media properly
- Adhere to strong authentication

Contact Information

We appreciate your feedback and comments. We can be reached at:

- Phone: 202-245-6252
- Email: Danny.Harris@ed.gov
- Fax: 202-245-6621

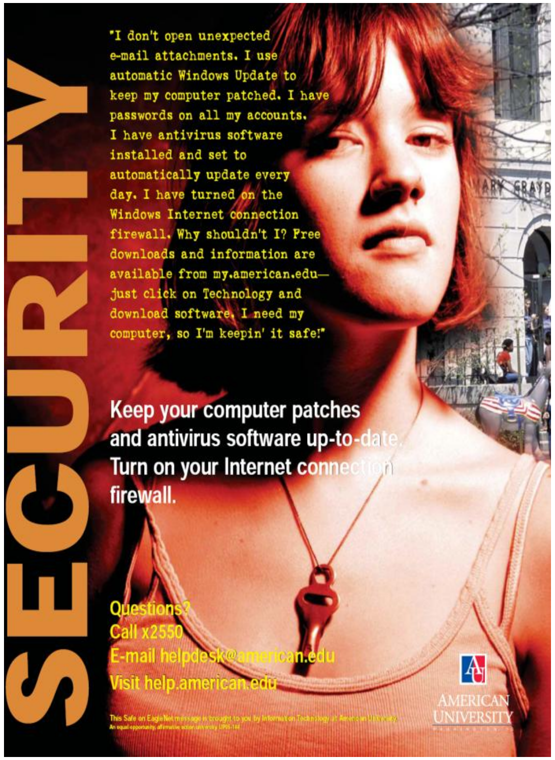
Session #50

A University's Perspective

Cathy Hubbs, CISO
Office of Information Technology
American University

Environment

- 11,000 Students (3,800 on campus)
- 2,600 Faculty & Staff
- Visitors, Parents, Alumni, Researchers, Guests
- iPads, iPhones, BlackBerrys, Laptops, Desktops, Servers, Windows, Mac, and *Nix
- Dual Data Centers – Business Continuity



"I don't open unexpected e-mail attachments. I use automatic Windows Update to keep my computer patched. I have passwords on all my accounts. I have antivirus software installed and set to automatically update every day. I have turned on the Windows Internet connection firewall. Why shouldn't I? Free downloads and information are available from my.american.edu—just click on Technology and download software. I need my computer, so I'm keepin' it safe!"

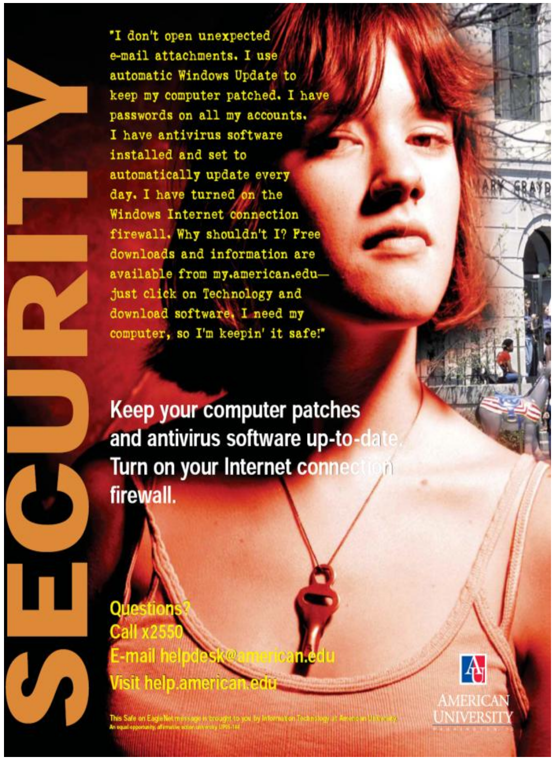
Keep your computer patches and antivirus software up-to-date. Turn on your Internet connection firewall.

Questions?
Call x2550
E-mail helpdesk@american.edu
Visit help.american.edu

This Safe on EagleNet message is brought to you by Information Technology at American University.
An equal opportunity, affirmative action university. UP05-144

Environment, cont.

- Compliance & Covered Data – Health, Student, Financial, Credit Card, Privacy Laws, Copyright, etc
- IT Security Team -> Move to ERM
- Institutional Review Board (research)
- Emergency Planning Group & Response Team
- General Counsel & Risk Officer partnerships
- Central IT and Tech Partners



"I don't open unexpected e-mail attachments. I use automatic Windows Update to keep my computer patched. I have passwords on all my accounts. I have antivirus software installed and set to automatically update every day. I have turned on the Windows Internet connection firewall. Why shouldn't I? Free downloads and information are available from my.american.edu—just click on Technology and download software. I need my computer, so I'm keepin' it safe!"

Keep your computer patches and antivirus software up-to-date. Turn on your Internet connection firewall.

Questions?
Call x2550
E-mail helpdesk@american.edu
Visit help.american.edu

This Safe on EagleNet message is brought to you by Information Technology at American University.
An equal opportunity, affirmative action university. UP05-144

Repeatable & Transparent Processes

- University Policy Template & Process
- Least Privilege – Data Custodians – Account Reviews
- Change Management
- Information Security Advisories
- System Development Life Cycle
  - Bake It In, Not Bolt On

Repeatable & Transparent Processes, cont.

- IT Services (ITIL) – SLAs, OLAs, MOUs
- Contract Review
- Risk Assessments | SharedAssessments.org
- Incident Response | Cyber Security MOU
- General Security Awareness

Technology - Depth in Defense

- Authentication & Health Check
- Whole Disk Encryption
- Patch Management
- Close Unused Ports/Services
- Central Logging
- Continuous Monitoring Web Applications

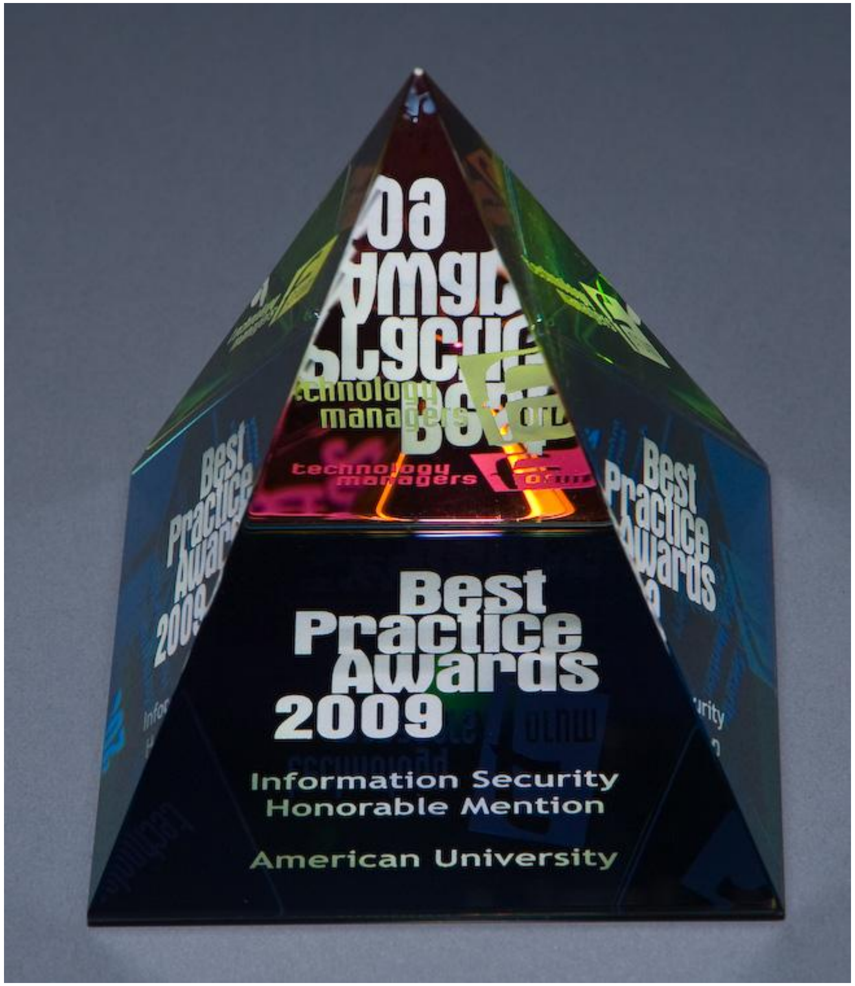
Technology - Depth in Defense, cont.

- Firewalls - Default Deny at Border
- Intrusion Detection/Prevention & Bandwidth Shaping
- Segmented and Redundant Network
- Spam/Phish Filters – Enforce Allowed Sender List

Contact Information

Cathy Hubbs, CISO
Office of Information Technology
American University

hubbs@american.edu
202-885-3998
security.american.edu


Best Practice Awards 2009
Information Security Honorable Mention
American University
technology managers forum

Session #50

Get Your Head Out of the Sand: You Have a Problem

Ira Winkler, CISSP

The Problem

- People think that the data they store is worthless to another person
- Protecting the data is not worth the effort
- The easiest data to steal is data that people don’t know is valuable
- The bad guys will come after the data the easiest way that they can get it
- You can never second guess the use of data by malicious parties

The Value of Data is Relative

- You have no idea what the intent of the bad guys is
- Inconsequential data to you can be extremely valuable to a third party
- The value might not be monetary
- The data can appear to be inconsequential to you

Frankly, It Doesn’t Matter What You Think

- It’s not your data
- If it is compromised, you are not the end victim
- Even if the data is completely worthless, the press will eat it up if it is a slow news day
  - “The private data of 100,000 students was stolen ….”
- Any efforts to minimize the extent of the compromise make you look worse

There is a Cost for a Compromise

- Investigations can cost hundreds of thousands of dollars
- Outages will cost money
- Data integrity must be examined
- PR nightmare and costs to mitigate bad press
- Class action lawsuits
  - They don’t care whether or not there was damage

Hidden Threats

- Abusive spouse wanting to locate spouse in hiding
- Manipulation of moneys owed
- Harassment of individuals by saying they owe more
- Identity theft
- Reuse of information for other purposes

There's No Such Thing as Worthless Data

- The intelligence process involves the collection of small pieces of data to put together the big picture
- Some data has more value than others, but when aggregated every piece has potential value

I Still Don’t Understand

- You are responsible for protecting the financial data, personal records and Social Security Numbers of students
- People will hack you just for your computers
- You have the personal information of millions of students
- What if someone stole your data?
- What if a woman was killed, because someone tracked her down through information stolen from you?

Yes, it happens

Compromises Happen All of the Time

- Even to companies who take security seriously
- Even to companies who do everything reasonable
- When, not if, you have a compromise, data will be assumed to be compromised

What are You Going to Do?

- This presentation covered the why, not the how
- There is no such thing as perfect security
- The expectation is reasonable security programs and countermeasures enacted proactively
- Protect student information
- Bad publicity hurts everyone

A Couple of Points to Consider

- You don’t know what you don’t know
  - Take reasonable steps, so at least you have a defensible position
  - Your current position may be indefensible
- Expect the worst to happen on a slow news day

Contact Information

I appreciate your feedback and comments. I can be reached at:

Ira Winkler, CISSP

- Phone: +1-410-544-3435
- Email: winkler@isag.com